EXECUTIVE SUMMARY

One year after the creation of the Department of Homeland Security (DHS), dangerous security gaps remain that place America at risk to the threat of terrorist attack. While we are safer today than we were before the September 11 attacks on our homeland, we are not as safe as we need to be to protect the American people from the threat of al Qaeda and like minded groups.

Our nation remains vulnerable to potentially catastrophic attacks involving nuclear, biological, chemical and radiological weapons. Pathways to the United States by land, sea and air are insecure. Our critical infrastructures have few defenses and our communities are not as prepared as they need to be to respond to a terrorist attack. We need to take faster and stronger action to close these security gaps. As the President has stated, we are at war, and therefore we must recapture the sense of urgency that existed in America two and a half years ago to protect our homeland.

We present this report in fulfillment of our constitutional obligation to vigorously oversee the Administration's homeland security efforts and our moral duty to recommend ways to make America safer. Summaries of many of the security gaps we have identified and our recommended solutions appear below. Some of the topics coincide with initiatives recently announced by the Department. We welcome these measures and will continue to work with the Administration and our colleagues in Congress to close the security gaps we face as soon as possible.

PREVENTING TERRORIST ATTACKS

Preventing Attacks by Improving Intelligence

Security Gaps:

- The DHS has still not completed a comprehensive threat and vulnerability assessment to set priorities and guide our strategy.

- The federal government has failed to develop a unified terrorist watch list accessible to border security personnel, state and local law enforcement, and others with homeland security responsibilities.

- The DHS's intelligence unit is still not functioning as intended; it is operating at less than 45 percent of its full strength.

Security Recommendations:

- The DHS should complete a comprehensive threat and vulnerability assessment as soon as possible, but no later than October 1, 2004.

- The Administration should exert the leadership necessary to complete a unified terrorist watch list as soon as possible.

- The DHS should complete its authorized hires of intelligence personnel so that the Information Analysis and Infrastructure Protection Directorate will be fully staffed and operational by October 1, 2004.

Preventing Attacks by Securing Nuclear Material

Security Gaps:

- Nuclear weapons and materials within the former Soviet Union and around the world are not secure and represent a direct threat to the United States.

- More than a dozen years after the break up of the Soviet Union, there are 105 nuclear sites within Russia and the former Soviet Union that need security improvements. They contain approximately 600 metric tons of nuclear materials, enough for about 41,000 nuclear warheads.

- Outside Russia, some twenty tons of highly enriched uranium exists at 130 civilian research facilities in 40 countries, many of which have no more security than a night watchman and a chain link fence.

- Domestic and international sources of radiological materials that can be used for a "dirty bomb" are also not secure. Federal investigators have documented 1300 cases in which radioactive material inside the U.S. have been lost, stolen, or abandoned over the past five years.

Security Recommendations:

- The Administration should follow the recommendations of the bipartisan Baker-Cutler Commission and triple resources dedicated primarily to securing nuclear materials and sites within the former Soviet Union.

- The United States should lead a global coalition to remove all vulnerable nuclear materials located outside the former Soviet Union and the Administration should increase its contribution to the Global Partnership Against the Spread of Materials of Mass Destruction.

- The Administration should identify vulnerable sources of radiological materials that could be used for a "dirty bomb" and takes steps to secure them. Licensing requirements should be tightened by ensuring that applicants are inspected before they may receive shipments of dangerous materials.

Preventing Attacks through Biodefense & Preparedness

Security Gaps:

- Dangerous stockpiles of biological agents developed by the former Soviet Union, as well as the human expertise built up in this, the largest and most intensive biological weapons program in history, are susceptible to theft or appropriation by terrorist groups. Security projects are underway at only four of 49 known biological sites with only two sites fully secured.

- Many U.S. facilities handling deadly pathogens have not had their security, inventories, and personnel reviewed, registered and certified by the government as required by law. The Administration missed (and then extended indefinitely) its own November, 2003 deadline for completing this review.

- Today, at least 57 different countermeasures are needed to defend against 19 of the major bioterrorist agents. Currently, only one of these countermeasures can be widely distributed. No vaccine is available for butulinum toxin, bubonic plague or tularemia. Virtually nothing has been done to address the growing threat presented by bioengineered pathogens.

- One year after the creation of DHS, there is still no comprehensive Biodefense Preparedness and Response Plan. Our public health infrastructure is poorly equipped to both detect and respond to a biological attack. Only six states have enough laboratory capacity to deal with a public health emergency and only two have sufficient workers to distribute vaccines in response to a biological attack. The National Smallpox Vaccination program has failed: it targeted the vaccination of 500,000 emergency workers and ten million first responders, only 39,000 have been vaccinated.

Security Recommendations:

- Efforts to secure weapons of mass destruction stockpiles around the globe should be tripled, consistent with the recommendations of the bipartisan Baker-Culter Commission and a portion of those funds should be dedicated toward securing biological stockpiles from the former Soviet Union.

- The Administration should make it a high priority to implement fully the legally mandated program to secure biological pathogen stocks in the United States.

- To develop the medicines and vaccines necessary to protect us, and the rest of the world, from bioterrorism, the United States should move beyond the limited confines of the Administration's "Project Bioshield" by developing robust, effective public-private partnerships for the development of new diagnostics, drugs, and vaccines. We must also move forward with the speed and resources reminiscent of the

Manhattan Project, in an effort to reduce the time necessary to move from "bug to drug" (pathogen detection to drug response) from years to a matter of weeks.

- The Administration should work in conjunction with state and local officials, health care providers, researchers and the private sector to develop a comprehensive Biodefense Strategy focusing on prevention, preparedness and response. This plan, which is long overdue, should be completed as soon as possible.

SECURING AMERICA BY SEA, LAND, AND AIR

Securing Our Ports

Security Gaps:

- The seven million cargo containers that arrive at American ports and move through our communities by truck and rail, only a small percentage of which are physically inspected or mechanically screened, represent a severe security threat as they are possible delivery devices for weapons of mass destruction.

- The vast majority of cargo containers that travel to and through the U.S. have no tamper resistant seals. The Administration has not established security standards for container seals.

- Millions of cargo containers are entering America without having been screened for radiological or nuclear devices.

- There are less than 100 inspectors currently assigned to foreign ports under the Container Security Initiative to screen the seven million cargo containers before they come to our shores. These inspection teams are unable to review all the manifests of cargo shipments headed toward the U.S.

- Of the 5,300 companies whose shipments receive reduced scrutiny at seaports due to their membership in the Customs-Trade Partnership Against Terrorism program (C-TPAT), only 130 have been audited and verified as meeting the program's security requirements.

- The Coast Guard has estimated that ports need to spend $1.1 billion this year, and $5.4 billion over ten years, to meet security standards set by the Coast Guard as instructed by Congress. The Administration's budgets since 9/11 have requested only $46 million for port security and although Congress has provided much more funding, there remains a $566 million funding gap for this year alone.

Security Recommendations:

- Radiation detection portals and other non-intrusive inspection technologies should be deployed in sufficient numbers to screen every cargo container entering America's ports and be integrated into normal port operations so they do not slow the flow of commerce.

- The DHS should require containers entering the U.S. to have a high security seal that meets international standards.

- The DHS should deploy robust inspection teams to the largest ports abroad and ports in high risk countries. Inspectors should be deployed for at least one year.

- All the companies in the C-TPAT program should be inspected by DHS to ensure that they meet minimum security requirements.

- Additional federal assistance is needed to meet short term security needs at America's ports this year. In the future, the federal government, ports, and industry should share the cost of providing robust port security.

Securing Our Borders

Security Gaps:

- There is only one border patrol for every 5.5 miles of our northern border. The Administration met its legal requirement to triple the number of border patrols on the northern border by moving hundreds of employees from the southern border. Staffing levels for border patrol, and customs and immigration inspectors are far below levels set by Congress and the Administration has not developed a new border staffing strategy for either the northern or southern border since September 11.

- Underinvestment in infrastructure impedes security programs, slows the flow of commerce and burdens the economies of border communities. A total of 64 land ports of entry have less than 25 percent of the required inspection space.

- Trucks entering the U.S. on the southern border are not comprehensively screened for nuclear or radiological materials. Tamper resistant seals are required on trucks crossing the southern border, but not the northern border.

- Citizens of 27 "visa waiver" countries are currently exempt from coverage of the US-VISIT system. Thus, people like the "shoe bomber" Richard Reed (a British national) and the alleged al Qaeda operative Zacarias Moussaoui (a French national) would not be fingerprinted and photographed under the US-VISIT system.

- Border security systems like US-VISIT are not currently linked to a comprehensive terrorist watch list.

Security Recommendations:

- The Administration should immediately develop and implement a comprehensive post-9/11 national border strategy that will allow DHS to effectively deploy its personnel and technology.

- The Administration should take advantage of this historic opportunity to revitalize our borders by investing in roads, other infrastructure, and inspection facilities that will allow for implementation of needed security programs while facilitating the legitimate travel and trade. The Administration should consider the full impact of US-VISIT on border communities and incorporate community representatives in the US-VISIT planning process.

- Radiation portal monitors should be installed immediately at all border crossings to support 100 percent screening of truck cargo for nuclear and radiological materials.

- Border security programs like US-VISIT should be linked to a comprehensive terrorist watch list as soon as it is completed so that border security personnel have real-time access to the most current watch list information available.

Securing Our Skies

Security Gaps:

- Despite massive expenditures, Transportation Security Administration (TSA) airport screeners continue to allow dangerous items to enter U.S. passenger planes.

- Most air cargo shipped on passenger planes is not screened for explosives. TSA does not audit the security practices of all the companies ("known shippers") permitted to place cargo on passenger aircraft.

- Passenger airliners have no defenses for surface to air missiles.

- Cargo aircraft that fly over the United States are not required to have hardened cockpit doors.

- Many airport employees are permitted to access sensitive areas of the airports without going through routine passenger screening.

Security Recommendations:

- The TSA should determine how many screeners should be deployed to ensure security and, if necessary, the artificial cap of 45,000 screeners should be lifted. TSA should provide more rigorous screener training and more frequent tests of the screening process.

- TSA should provide greater security for air cargo on passenger aircraft, with the goal of 100 percent inspection as soon as possible. The security practices of all "known shippers" should be verified.

- The DHS should develop and deploy as soon as feasible, technology that can protect passenger airliners from attack by shoulder fired missiles.

- Cargo flights passing over the United States should be required to have hardened cockpit doors.

- All persons who enter areas beyond the screening checkpoint should be screened for dangerous items.

PROVIDING SECURITY INSIDE AMERICA

Protecting America's Critical Infrastructure

Security Gaps:

- America's chemical facilities, food supply, water systems, telecommunications facilities, electrical grid, energy plants, pipelines, roads, bridges, tunnels, dams, subways systems, hospitals, skyscrapers and arenas are all potential targets for terrorist attacks – yet the Administration has not taken strong action to secure even the most vulnerable and dangerous of these critical infrastructures, relying too heavily on voluntary private action.

- The Administration has not completed a comprehensive risk assessment to identify our greatest vulnerabilities and prioritize implementation of protective measures. One senior DHS official estimated that completion of such a study would take five years.

Security Recommendations:

- The Administration should explore tax and other incentives to increase infrastructure security, speed the development of commercial products like terrorism insurance, and as necessary, develop a minimum regulatory framework that does not place unreasonable demands on business owners, such as requirements to undergo periodic vulnerability assessments and security audits.

- The Administration should complete, as soon as possible, but no later than October 1, 2004, an initial national critical infrastructure risk assessment. The recent announcement that DHS will create a national database of critical infrastructure is but the first step toward the development of a genuine infrastructure risk assessment.

- The Administration should establish an annual, sector-by-sector report card and awards program recognizing significant improvements or achievements in critical infrastructure protection.

Protecting Chemical Plants

Security Gaps:

- Today there are 123 chemical facilities in the U.S. that could threaten over one million people in the event of a massive breach of chemical containment due to a terrorist attack.

- Unlocked gates, absent guards, dilapidated fences and unprotected tanks filled with deadly chemicals occur at dozens of plants across the country.

Security Recommendations:

- The Administration should require all facilities that pose a substantial danger to conduct vulnerability assessments, develop security plans to address vulnerabilities and submit these plans to DHS by October 1, 2004.

Protecting Cyberspace

Security Gaps:

- There is no senior level official in the Administration who has the explicit authority to direct the multiple agencies necessary to prevent and respond to a cyber-9/11. There is no central organization through which officials from the federal government and private industry can coordinate and respond to a cyber-crisis.

- Government computer networks are insecure. Eight of the agencies surveyed received failing grades on their cybersecurity from the House Government Reform Committee. The DHS received the lowest score: 34 of 100.

- Home computer systems are also vulnerable and can be used as launching points for "distributed denial of service" and other attacks. These attacks are causing billions in damages.

Security Recommendations:

- A new senior level official for cybersecurity should be designated who will report directly to either Secretary Ridge or the President.

- The Administration should create a National Crisis Coordination Center that could house, within a single facility, representatives from the private sector, federal, state and local government agencies who can bring relevant parties together in the event of a cyber-9/11.

- All government agencies should require that the software they purchase is preconfigured with the highest level security settings.

- A Chief Security Officer should be appointed in the Office of Management and Budget to coordinate the federal government's efforts to secure its computer systems.

- The federal government and the private sector should establish a framework specifying the actions that each should take to help individual computer users to secure their systems.

Protecting the Food Supply

Security Gaps:

- The FDA currently inspects only two percent of food imports under its jurisdiction. USDA's one percent increase in inspectors at food facilities is insufficient in light of the severity of the threat.

- Lab testing capacity necessary to rapidly detect threats to agriculture and food does not exist in every state.

- The Administration does not yet have a national response plan for preparing and defending the nation against catastrophic attacks on our agricultural system or food supply.

Security Recommendations:

- USDA, FDA, and DHS should deploy additional food inspectors to our borders and food processing and packing plants.

- At least one lab in every state should have the capability to conduct tests for key agro-terror threats.

- The DHS should take the lead in developing a comprehensive national agro-terrorism response plan within the next year that contains specific goals and timetables for achieving those goals.

Protecting America with Information Technology

Security Gaps:

- By merging 22 agencies together, DHS inherited as many as 8,000 information technology applications, one hundred of which are considered "major." Yet, DHS has not harmonized basic systems to manage the department, like accounting, procurement, grant management, and budgeting. In many instances, benefits and payroll continue to be provided by legacy agencies. According to a DHS senior official, DHS keeps a "running hand-tallied list of its staff, with the total varying from 190,000 to 225,000 depending on which of the 22 component agencies' 24 human resources systems are consulted."

- The Administration is not taking advantage of information technology for homeland security needs in key areas such as information sharing across agencies and with state and local governments. The Markle Foundation concluded that "the government's progress toward building an adequate network has been slow and is not guided by an overall vision."

Security Recommendations:

- The Administration should make extensive use of the most up-to-date information technologies to improve homeland security functions and unify DHS into a more cohesive organization. The DHS should establish clear milestones and timelines for completing its major information technology initiatives.

- Management and procurement of information technology need to be strengthened by increasing the authority of the Chief Information Office and Chief Procurement Officer.

- The DHS should create an information technology "red team," which includes leading private sector experts, to advise the Department on how to speed integration of its information technology infrastructure and plug critical gaps in current systems.

PREPARING OUR COMMUNITIES

Preparing Our Nation's First Responders

Security Gaps:

- Two and a half years after the attacks of September 11th, many first responders still lack interoperable communications equipment and cannot communicate with one another. The Administration has allocated no new funds in its proposed fiscal year 2005 budget to address the issue.

- The DHS has still not established a set of essential capabilities that all communities should have, based on the threats and vulnerabilities they face, to respond to terrorist attacks. Despite the expenditure of billions of dollars, we have no way to measure how and whether we are adequately preparing to protect communities throughout America.

- Federal grant programs are not getting money to our communities quickly enough. Distribution of funding is based on arbitrary formulas rather than the risks that communities face – California, New York, Texas and Florida received about $6 per capita while states like Wyoming, North Dakota, and Vermont received over $30 per person.

Security Recommendations:

- Technologies that provide short-term, baseline communications already have been identified by state and local officials. The DHS's recent announcement that it will provide "technical specifications" for these systems is nothing new. Rather than re-identifying these technologies, DHS should provide a dedicated, annual funding source to assist communities in deploying affordable, existing technologies that would enable first responders to communicate at the scene of a disaster right now.

- The Department should determine the essential capabilities necessary for first responders to protect every community in America, and then make the commitment to obtain these capabilities and provide first responders with the tools they need to do their jobs.

- Grant programs should be consolidated and revised as proposed in bipartisan legislation before the Select Committee on Homeland Security. Funding should be based on an assessment of threats and vulnerabilities, not formulas.

PRESERVING OUR VALUES

Reinforcing Security, Privacy, and Civil Liberties

Security Gap:

- In the past year, homeland security initiatives, such as data mining efforts and an airline passenger screening system, have been derailed or postponed because the Administration has failed to adequately evaluate the programs' effects on privacy and civil liberties.

Security Recommendations:

- The Administration should create a Chief Privacy Officer responsible for evaluating privacy issues that arise in conjunction with the development and use of new technologies in the federal government. Congress should consider creating offices like the DHS Privacy Office in other agencies with substantial homeland security responsibilities.

- The Administration should create a Commission on Privacy, Freedom and Homeland Security to evaluate the implementation of homeland security initiatives in a way that reinforces our fundamental constitutional rights and values.